i春秋安全勇士--一些简单题wp

原创

xuqi7 于 2016-07-08 09:39:51 发布
分类专栏： ctf

基础题60分

用firebug可以发现一段奇怪的js，

把eval改成alert，运行之后再改一下，最后会就是冒号隔开的一串数

然后改下格式 \x30 这种，然后转16进制，然后是md5解一下就可以了

培根

我*年*轻时*注*意到，*我*每做十*件事*有九件*不成*功，于是我就十倍*地*去努力干下去。—— 萧*伯纳*

ABAABAABAAABBAAABBAAAAAAABAAAAAAABB

正常培根解出即可

Base64

Base64的脚本，

```
#! usr/bin/env python

# -*- coding:utf-8 -*-

import base64

import string



a="6ZWc6Iqx5"

b="C05pyI"

c=["a","b","c","d","e","f","g","h","i","j","k","l","m","n","o","p","q","r","s","t","u","v","w","x","y","z",

for i in c:

        printbase64.b64decode(a+i+b),I,a+i+b
```

填镜花水月 对应的 base64编码就可以了

渗透测试_80pt

看源码发现k的长度是400px，而且题目为flag是弹出来的，于是构造k为：

400个a +一个空格+<script>alert(1);</script>

（其实不用这样，直接写js代码就好了…）

渗透测试_100pt

龙神的思路：根据提示可想到文件包含漏洞，测试发现可以这样利用

file=php://filter/read=convert.base64-encode/resource=index.php

发现没什么内容，然后用御剑扫一下目录

发现有index.php，1234.php

看一下1234.php，内容base64解码即可

流量分析_100pt

龙神的思路：wireshark打开，然后 文件-->导出对象àhttp,

得到一堆asp页面，然后打开就找到flag了，在9,11中都可以找到

渗透测试_150pt（之前做过这题，忘了….）

Firebug看了下过程

先是login.php，然后是admin.Php，提示权限不足后跳回index.php

在admin.php中，响应返回中有

Set-cookie:token=deleted

有一个cookie：token=ad0234829205b9033196ba818f7a872b

Md5解密之后是test2（之后就是明神提示我）

之前做的时候就是各种猜测，在用户名，密码框输各种东西，后来才知道把cookie改了就好了，用fiddler把cookie改成admin1的MD5值，然后提交，还有一个坑是3秒之后会重定向到登录页面，我之前设置过火狐不允许自动重定向，所以没坑到我，而且我是用fiddler抓包看的，直接就看到flag了（机智）

流量分析_200pt

稍微看了下，发现用户名as，密码asss，还有人在sql注入

不想看了，就想导出一下，没什么用（其实有用，这题太弱智，直接搜flag就可以了）

之后又用foremost提取，一堆网页，在最后一个网页里发现flag

流量分析_300pt

一开始很容易从数据包中分出一张中国地图…..

之前还找过几个exif信息，但是没用

还是从这张图片入手吧，有水印：www.ynbsm.gov.cn

然后访问一下，发现是云南，那就看看地图上的云南区域，发现真的有东西

看不太清，用ps来处理下，图像-à调整—>黑白

这样就看的比较清楚了，也就知道了flag

flag{@G00d_L4ck_H3r3@}

（其实一开始分离出这么大的图，就应该能想到）